Peter C. Hildreth
Bank Commissioner

Robert A. Fleury
Deputy Bank Commissioner

64B Old Suncook Road
Concord, NH 03301

Phone (603) 271-3561

Division FAX Numbers:
Banking (603) 271-1090
Consumer Credit (603) 271-0750

The
BANKING DEPARTMENT NEWSLETTER
FALL 2005

www.nh.gov/banking

Volume 4 • Issue 4

FROM THE COMMISSIONER'S DESK

As 2005 ends, we all tend to look back on the important events that occurred over the year. And, we also look ahead to a busy and challenging 2006!

As you can imagine, it was a very busy and productive year for us in the Banking Department. While there were many high points in the year, several of them happened since our last newsletter.

In what I believe were first time events, Governor John H. Lynch hosted receptions for bank senior staff and for credit union management. Both sessions were held at Bridges House, the "official" governor's house, located in East Concord. The events allowed for informal as well as formal conversations with the Governor. Many of those who attended told me how much they enjoyed the event. Governor Lynch has told me that he too enjoyed meeting the leaders of our institutions. He also mentioned that the information he received was helpful to him as Governor.

In the fourth quarter, the biggest good news, at least for licensees of the Consumer Credit Division, was the inauguration of online license renewals. The system is a big hit with our "customers." One mortgage broker told me he renewed his license during half time of a football game and still caught some of the show! As of December 14, 2005 sixty-eight percent (1,238 out of 1,814) of all licenses have been renewed using the online process. It should be noted that ninety-one percent of the companies that requested the online credentials have renewed online.

Credit for this successful project goes to:
Mary Jurta, Director of Consumer Credit
Dawn Allen, Director of Operations
Celeste Couture, Licensing Supervisor
Theresa Moulton, Program Specialist
Janice Schultz, IT Manager, Office of Information Technology
And all employees of the Consumer Credit Division.

Looking forward, I expect that 2006 will be as busy and as challenging as 2005. We at the Banking Department look forward to working with all of you in the New Year. We hope your holiday season, whichever holiday you celebrate, will be filled with good times spent with family and friends.

COMMISSIONER HILDRETH JOINS CSBS BOARD OF DIRECTORS

Commissioner Peter C. Hildreth has been appointed to the Board of Directors of the Conference of State Bank Supervisors (CSBS). He was nominated by current CSBS Chairman Eric McClure, Commissioner of the Missouri Division of Finance.

"I look forward to working with CSBS in the many national issues facing community banks and state bank regulators," Hildreth said.

CSBS is the national organization of state officials responsible for chartering, regulating and supervising the nation's 6,300 state chartered commercial and savings banks and over 400 state-licensed branches and agencies of foreign banks.

Legislative Update

Donna M. Soucy – General Counsel

New Rules Adopted: Credit Union Amendments to By-Laws & Branching

The Department recently adopted new rules relative to the amendment of credit union bylaws and interstate credit union branching. The rules Ban 1107 & Ban 510.09, which became effective on November 11, 2005, provide a petitioning process for those credit unions who seek to amend their bylaws or establish a branch in another state.

Ban 1107 sets out specific requirements for those credits unions who wish to amend their bylaws for qualification of membership. Specifically, credit unions, who seek to make changes in their qualification for membership will now need to provide the Bank Commissioner with a business plan detailing the following:

(1) The benefit to the credit union of the change in qualification of membership;

(2) A plan for delivery of services to the new membership;

(3) A procedure for verifying that individuals meet the requirements for qualification for membership; and

(4) A demonstration of the credit union's financial ability to complete the plan.

Upon submission of a complete petition but not before the completion of a 30 day notice period, the Commissioner shall grant or deny the petition.

Also, Ban 510.09 with the written approval of the Commissioner, permits New Hampshire chartered credit unions to branch into host states provided that the host state's law reciprocally permits New Hampshire to act as a host state for branches of its home state chartered credit unions.

BANKING DIVISION NEWS

Charles M. O'Connor – Chief Bank Examiner

New State Chartered Entity

On October 17, 2005 the Bank Commissioner authorized Pyramis Global Trust Company, Merrimack, N.H. to open as a non-depository trust company.

Annual Reports

The 2005 Annual Report forms are available on the department's website. The form is available in Word and PDF for your convenience. If you need more space then is allocated please put "See Attached" in the first row and attach an additional paper with the required information.

Please remember that original signatures are needed on all forms that require a signature. All forms should be typewritten originals, authenticated copies, or computer duplicates. All filings need to be received by our office on or before January 29, 2006. A statutory fine of $25 per day will be assessed for each day delinquent.

If you have any questions do not hesitate to contact Chief Bank Examiner Chuck O'Connor.

Account Information At-a-Glance

We send out a reminder letter regarding the form (NHBD-10) in December and June. Submission of the form is required by all state chartered depository institutions by January 1st and July 1st of each year. BAN 705, available on our website, is the governing regulation. In addition, the form is required to be posted in the lobby of the institution's main office as well as all branches. The form is available on our website and the completed form can be emailed to **NHBD@banking.state.nh.us** or mailed in.

Interest on Escrow Accounts

A reminder letter is mailed in December and June of each year to all state chartered depository institutions. From the information received, we calculate the interest rate payable on escrow accounts for the next six month period. RSA 384:16-c and RSA 384:16-e, available on our website, are the governing laws. The form is available on our website and the completed form can be emailed to **NHBD@banking.state.nh.us** or mailed in.

Duties of a Directed Trustee

By Chris Blanchette, Bank Examiner IV

The fiduciary responsibilities of a directed trustee have been traditionally very limited to executing directions and transactions provided by the named fiduciary in employee pension plans. However, several recent events and court decisions have focused increased attention on the nature and scope of a directed trustee's fiduciary duties. There is still the distinction that a directed trustee's duties are significantly narrower than a discretionary trustee; however, a directed trustee's actions may be under more scrutiny given the fiduciary responsibilities that must be followed.

The Department of Labor (DOL) issued Field Assistance Bulletin (FAB) 2004-03 on December 17, 2004 to provide some guidance and clarification regarding the responsibilities of a directed trustee under the Employee Retirement Income Security Act (ERISA). ERISA describes a plan trustee as always being a fiduciary because the plan trustee exercises authority or control over the plan's assets. Section 403(a)(1) of ERISA details situations whereby a trustee may have limited authority; however, it does not preclude a directed trustee from meeting the requirements of ERISA. Under Section 403(a)(1), the directions carried out by a directed trustee are considered to be "proper" only if the direction is made in accordance with the terms of the plan. Additionally, a direction received must be in accordance with ERISA. Accordingly, if the directions received from a plan fiduciary are not made in accordance with the terms of the plan or is contrary to ERISA, the directed trustee may not prudently follow the direction.

In order to ensure all fiduciary responsibilities are being met, trust companies who act in a directed trustee capacity need to perform due diligence to the degree necessary. Copies of all relevant documents and governing instruments should be obtained and reviewed in order to make that determination of adherence to all fiduciary responsibilities. A directed trustee may be liable for following a non-compliant direction on the basis that the directed trustee "should have known". A directed trustee may also be liable for a breach of fiduciary duty to follow proper directions. The FAB does allow for the directed trustee to rely on the interpretation from the plan fiduciary in certain circumstances.

Nonetheless, the discretionary trustee continues to have the primary responsibility for determining the prudence of transactions in the plan. Recent developments have continued to support the recognition of a very limited scope of a directed trustee's responsibilities. Additionally, it is not expected that a directed trustee have an obligation to determine the prudence of every transaction, nor does it have the obligation to second guess the decisions of discretionary trustees. The obligation is to make sure the directions are proper and are made in accordance with the plan and are not contrary to ERISA. Refer to FAB 2004-03 which can be

found at **www.dol.gov** for further information. The bulletin further describes the directed trustee's responsibilities with respect to its duties to act on non-public and public information, as well co-fiduciary responsibilities.

Information Security – The Quick and the Dirty

By Parker T. Howell, Bank Examiner III

Introduction

This is the first article in a series dealing with Information Technology (IT). These articles are meant to provide additional guidance to financial institutions in the area of IT management best practices, but will primarily focus on information security. Topics covered in future newsletters will include patch management, disaster recovery, vendor management, network security, access controls, IT risk management, and remote access just to name a few.

Everyday we hear of lost or stolen customer information, security breaches, account hijacking, and phishing scams. Information security or insecurity is more prevalent today than ever before and financial institutions must be proactive in protecting their customers' and members' sensitive information. To help ensure that this was done, Congress passed the Gramm-Leach Bliley Act (GLBA) in 1999. The GLBA requires all financial institutions to develop, implement and document an information security program. This article will discuss the who, what, why, when, and how of information security.

What

Several definitions exist for information security. The requirements set forth in (GLBA) Appendix B part 364 of the FDIC rules and regulations, and Appendix A part 748 of the NCUA Rules and Regulations states this about information security:

"A comprehensive written information security program includes administrative, technical and physical safeguards…and should be designed to ensure the security and confidentiality of customer/member information; protect against any anticipated threats, or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer/member."

Why

Financial institutions must protect their most valuable asset - customer information. Reputational costs of a major security breach could be so high that the institution may be unable to recover. The banking industry is founded upon consumer confidence. If security breaches and identity theft become increasingly prevalent, what are the long term effects to the industry as a whole? Would it be a stretch to think that those with stronger security programs may have a competitive advantage?

Who

Information security is the responsibility of everyone! The old saying that "you're only as strong as your weakest link" holds true when it comes to security. For instance, it takes only one employee to empty confidential information into the wrong trash can to create a security breach.

Ultimately, the Board of Directors is responsible for developing an information security program. They are required by GLBA to oversee the development, maintenance and implementation of the information security program. It is management's responsibility to enforce board policy and ensure that all employees understand their role. All employees need to understand the importance of information security as well as the underlying significance of security and the specific security-related requirements expected of them.

How

Developing and implementing a security program is a continuous process. Management and the board should identify what assets need protection, decide how to protect them, test protective measures to determine effectiveness, and adjust the program accordingly. If anything changes then the process should start over. This is most important as management offers new products, processes change, and new vulnerabilities are introduced. We will call this the information security cycle. I have broken it down into four basic steps.

1. *Perform Risk Assessment*

   The first step in developing and implementing a security program is to perform a risk assessment. The risk assessment allows you to identify the assets that you are trying to protect and the threats to those assets. Once you have identified assets that need protection you can design safeguards to protect those assets.

2. *Design Safeguards*

   Safeguards or controls, can include administrative (policy/ procedures), technical (passwords, firewalls) and physical (door locks) safeguards. A good program will incorporate all three into what is called a "layered approach". Safeguards can also be classified as preventative, detective, and corrective. For instance, a lock on the computer room door would be a preventative safeguard, while the surveillance camera above would be a detective safeguard. A corrective safeguard may be incident response procedures to review the surveillance tapes. Once again, a good program will have elements of all three; however, preventative safeguards should receive the most attention.

3. *Test Safeguards*

   What good is a safeguard if it is ineffective? Testing safeguards is a critical process in the information security cycle. Testing most frequently occurs through

audit, penetration testing and vulnerability assessments. If testing shows inadequacies then management should take action to put proper safeguards into place.

4. *Adjust the Program*

   Now that you have identified risks, designed safeguards, and tested the safeguards it is time to revisit the risk assessment to determine if new risks have been presented to the institution. New risks are introduced as new products are offered, new systems are put into place, and processes change. In addition, new vulnerabilities to computer systems are being discovered every day. This is where patch management becomes increasingly important. (Topic for another day).

When

The time to implement an information security program is now! GLBA compliance was required by July 1st 2001.

GLBA

The GLBA requires financial institutions to develop, implement, and document an information security program. GLBA outlines several steps that are needed for compliance. The steps above are functional and are requirements for an information security program; however, these steps alone do not satisfy the requirements of the act. Additional steps needed include specific assignment by the board for program implementation, annual training, vendor oversight requirements, and annual reporting to the Board of Directors on the program's status.

Summary

That's information security in a nutshell. Of course implementing and testing safeguards or controls can be extremely expensive, but so could one major security breach. In addition, information security is no longer just a "best practice", it is a requirement. New vulnerabilities are discovered everyday, and they are only going to become more prevalent as institutions find new ways of servicing their customers. The goal of the program is to identify and mitigate the vulnerabilities before they become problematic.

For more information see the *Information Security Handbook* at **www.ffiec.gov**

Debit Cards

By Anne J. Rabuck, Staff Attorney

Many individuals have commented to the department that they were unaware that when they use their debit cards at the gas pump, gas stations may temporarily charge a fixed amount, even if this amount exceeds the amount of the actual purchase. Some fixed amounts are set at $75 or $100. Adjustments to this fixed amount which reflect the actual amount charged are not made, in some cases, for three days.

It might be helpful if institutions included a statement stuffer which points out to customers that when a debit card is used, there is an advantage to paying inside the gas station (not at the pump) so that the PIN may be used and the exact amount of the charge can be deducted from the customer's account. This way, no hold is placed on the account.

CONSUMER CREDIT DIVISION NEWS

Mary L. Jurta, Director of Consumer Credit

Several years ago, under the guidance of a new Banking Commissioner, Peter C. Hildreth, the Department began a process to streamline its regulation and reduce regulatory burden for its licensees including Retail Sellers, Sales Finance Companies, Mortgage Brokers, Mortgage Bankers, Mortgage Servicing Companies, Small Loan Lenders, and Debt Adjusters. The changes began with the laws, making them uniform in basic licensing and state regulatory requirements, and having only their unique responsibilities, especially under federal law and regulations, vary among the types of licensed companies.

One of the results of this effort is that for the first time, this year, the Consumer Credit Division of the Department was able to offer an online renewal process to its licensees. Approximately ninety-one percent of all licensees issued credentials used the system. We have had very positive feedback from our licensees and we hope to bring future improvements to our database system to allow companies to report other information and changes directly online in the future.

The next deadline that looms for most licensed companies (mortgage bankers and brokers, sales finance companies, small loan lenders and debt adjusters) is the filing of the annual report. The annual report of business conducted by the licensed company during calendar year 2005 is due to be filed and received by this office on or before Wednesday, February 1, 2006. Report forms will be sent to all companies and will be made available on-line at our website, **www.state.nh.us/banking** by January 1, 2006.

As part of the annual report mortgage companies are required to report the names of all originators who originated NH loans during 2005. The Banking Department will send each mortgage company a report of originators as reported by the company on last year's annual report. This will allow the company to see what the Department has on file and will allow the company to edit the information to update it. This process will not be available for online filing this year, but we anticipate online filings of annual report next year.

Information about originators includes their complete name, last 4 digits of their Social Security Number, the date that they started working with the company ("start

date"), and the date they terminated with the company ("end date"), if applicable. The data provided by us to the company will only show "active" originators as of December 31, 2004 (those originators who the company reported as still working for them through that date, the last date of the reporting period; any originator terminated prior to December 31, 2004 would have had an "end date" on last year's report and will not be included in the list). The mortgage company can then update the list by entering appropriate "end dates" for originators no longer work for or originate for the company, and by entering the names, last 4 digits of SSNs and the "start date" for each originator not on the list who worked or originated for the company during any time of calendar 2005.

In closing, we would again like to remind all companies (except retail sellers) to make sure to file a copy of their financial statements within 90 days of the company's fiscal year end. Companies should file audited financial statements, if available. If audited financial statements were not prepared, the company must prepare a financial statement in accordance with generally accepted accounting principles with appropriate note disclosures. A mortgage banker, sales finance company, small loan lender and debt adjuster must file a financial statement that includes a balance sheet, income statement, statement of changes in owners' equity and a cash flow statement. A mortgage broker's financial statement shall include a balance sheet or a statement of net worth. In all cases, if the financial statement is not audited, a certification statement shall be attached and signed by a duly authorized officer of the licensee. The certification statement shall state that the financial statement is true and accurate to the best of the officer's belief and knowledge.

Please note that filing the financial statements of a licensee's parent company or consolidated financial statements **do not** fulfill the requirements under the statute. Financial statements must reflect the business activities and assets of the licensee itself.

Annual Report Update

Please note: The Department is enforcing the requirement to file a timely, and ***accurate*** annual report. See RSA 397-A:13. Fines will be levied when the Department discovers that the work papers (which must be maintained by law) for annual reports do not support the annual report filed with the Department in addition to requiring the licensee to submit an amendment.

Fair and Accurate Credit Transactions Act of 2003 – Final Rule Regarding the Disposal of Consumer Report Information and Records

By Andrea J. Shaw, Staff Attorney

Privacy issues are on the forefront of today's electronic society. Legislators have this issue in mind when they pass new legislation requiring regulatory agencies to promulgate new regulations intended to ensure consumer's personal information is handled in an appropriate manner that corresponds to the information's sensitivity level. Legislators and regulatory agencies appear to be striving to require businesses to treat social security numbers with more protections and cautions than publicly available data, such as your address. This article discusses one of the specific privacy regulations promulgated by the Federal Trade Commission's (hereinafter "FTC") addressing requirements for disposing of consumer credit reports and records derived from such reports.

The FTC final rule implementing section 216 of the Fair and Accurate Credit Transaction Act ("FACTA") became effective June 1, 2005. The rule requires "any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal." 16 CFR 682.3. The rule continues on to provide examples of reasonable measures to protect against unauthorized access to consumer information when that information is discarded. 12 CFR 682.3(b). The inherent flexibility in this standard is necessary to allow businesses to function and account for the increase in cost of additional regulatory protections. There is a higher cost to sending all your documents to a secure document destruction company, than if you choose to only send items that contain "more sensitive" information (refer to the social security / address example above). The flexibility allows each business to make its own decisions as to the most efficient way to deal with the disposal of the varying degrees of sensitive personal information it holds from consumers.

While the rule's standard is flexible, to whom it applies is not. The rule specifically applies to "any person" (meaning any individual or entity) that falls under the jurisdiction of the FTC. The rule covers a broad range of entities and business types, including, but not limited to: " consumer reporting companies; lenders; insurers; employers; landlords; government agencies; mortgage brokers, car dealers; attorneys; private investigators; debt collectors; individuals who pull consumer reports on prospective home employees, such as nannies or contractors; and entities that maintain information in consumer reports as part of their role as a service provider to other organizations covered by the Rule". **http://www.ftc.gov/opa/2005/06/disposal.htm** 11/14/05. For Consumer Credit Division ("CCD") purposes, all licensees are subject to this rule.

Last, if your business is subject to the Gramm-Leach-Bliley Act and the FTC's Standards for Safeguarding Customer Information, this disposal rule's flexible standard should be able to be nicely incorporated into your existing information security programs.